REMARKS

Claims 1-3, 5-11 and 13-27 are currently pending in the subject application and are presently under consideration. The below comments present in greater detail distinctive features of applicants' claimed invention over the cited art that were conveyed to the Examiner over the telephone on January 17, 2008.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments herein.

I. Rejection of Claims 1-5, 9, 10 and 12-27 Under 35 U.S.C. §102(b)

Claims 1-5, 9, 10 and 12-27 stand rejected under 35 U.S.C. §102(b) as being anticipated by Stallings, William. (Cryptography and Network Security; Third Edition. Chapter 9/Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems. Upper Saddle River, NJ. Prentice Hall, 2003. Pgs. 259-265, 290-293, 444 and 655). Withdrawal of this rejection is requested for the following reasons. The cited reference fails to disclose or suggest all aspects set forth in the subject claims.

> A single prior art reference anticipates a patent claim only if it ***expressly or inherently describes each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.,* 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The ***identical invention must be shown in as complete detail as is contained in the … claim***. *Richardson v. Suzuki Motor Co.,* 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

The claimed invention provides methods and systems facilitating the exchange and use of a session key to facilitate secure communication. To this end amended independent claim 1 recites *a message encryption system comprising: a session key employed to securely exchange a message associated with a dialog; and, an encryption component that employs asymmetric encryption to first securely transmit the session key,* ***the session key thereafter being employed to encrypt the message and securely exchange the message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the***

message. Independent claims 14, 18, 22, 26 and 27 recite similar features. Stallings is silent regarding such novel features.

Stallings relates to principles of public-key cryptosystems and secret key distribution with confidentiality and authentication. At page 4 of the Final Office Action, the Examiner contends that Stallings discloses such novel features. Applicants' representative avers to the contrary. In accordance with the claimed invention, the initiating user generates a session key, encrypts it with a private key associated securely with the initiator and a public key associated with a recipient and then sends the encrypted session key to the recipient. The recipient decrypts the session key in the reverse order, first using his private key, then the public key of the initiator. Subsequent messages in a dialog sent from the initiator are encrypted twice, initially with the session key, the encrypted message is again encrypted with the private key of the initiator. The recipient decrypts these messages first with the public key of the initiator, then the session key. At the cited portions, Stallings discloses a secret key distribution that provides protection against both active and passive attacks. A secret key is encrypted using the private key-public key pair and passed from an initiator to a recipient. The encrypted message containing the secret key is decrypts the message to recover the secret key (fig 10.6 and text at p.292 lines 23-27, p.293 lines 1-11). At the cited portions at pg. 444 lines 19-21, Stallings discloses that each session key is associated with a single message and is used for encrypting and decrypting the message. However, Stallings is silent regarding further encrypting the encrypted message with a private key of the sender. Further, at the cited portions of pg. 265 lines 15-17, Stallings discloses in another embodiment the aspects of public-key cryptosystems, where public-key systems consist of a cryptographic type of algorithm with two keys, one held private and one available publicly. Depending on the application, the sender uses either the sender's private key or the receiver's public-key, or both to perform some type of cryptographic function. Public-key cryptosystems are further classified into 3 categories, where the sender encrypts a message with the recipient's public key, the sender signs a message with its private key and the two sides exchange a session key. This private key used to digitally sign the message is part of the public-key system that is held private by the sender. In contrast, the claimed invention allows messages in a dialog sent from the sender to be encrypted twice, initially with the session key, the encrypted message is again encrypted with the private key of the sender. Thus, Stallings is silent regarding ***the session key thereafter being employed to encrypt the message and***

securely exchange the message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message as recited by the subject claims. Accordingly, it is requested that this rejection with respect to independent claims 1, 14, 18, 22, 26 and 27 should be withdrawn.

II. Rejection of Claim 11 Under 35 U.S.C. §103(a)

Claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings. It is respectfully requested that this rejection be withdrawn for at least the following reasons. Claim 11 depends from independent claim 1. As discussed *supra*, Stallings does not teach or suggest all aspects of amended independent claim 1. Accordingly, it is requested that this rejection be withdrawn.

III. Rejection of Claims 6-8 Under 35 U.S.C. §103(a)

Claims 6-8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings in view of VanHeyningen *et al.* (US 2002/0112152). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Stallings and VanHeyningen *et al.* do not teach or suggest all aspects set forth in the subject claims. Claims 6-8 depend from independent claim 1, and as discussed supra, Stallings does not teach or suggest all aspects recited by amended independent claim 1. VanHeyningen *et al.* discloses methods and apparatus for providing secure streaming data transmission facilities using unreliable protocols and does not compensate for the aforementioned deficiencies of Stallings. Accordingly, it is respectfully submitted that this rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP566US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731